Chapter 40
Utah E-Commerce Integrity Act

Part 1
General Provisions

13-40-101 Title.

This chapter is known as the "Utah E-Commerce Integrity Act."

Repealed and Re-enacted by Chapter 200, 2010 General Session

13-40-102 Definitions.

As used in this chapter:

(1)
(a) "Cause to be copied" means to distribute or transfer computer software, or any component of computer software.
(b) "Cause to be copied" does not include providing:
(i) transmission, routing, intermediate temporary storage, or caching of software;
(ii) a storage or hosting medium, such as a compact disk, website, or computer server through which the software was distributed by a third party; or
(iii) an information location tool, such as a directory, index, reference, pointer, or hypertext link, through which the user of the computer located the software.

(2)
(a) "Computer software" means a sequence of instructions written in any programming language that is executed on a computer.
(b) "Computer software" does not include a data component of a webpage that is not executable independently of the webpage.

(3) "Computer virus" means a computer program or other set of instructions that is designed to degrade the performance of or disable a computer or computer network and is designed to have the ability to replicate itself on another computer or computer network without the authorization of the owner of the other computer or computer network.

(4) "Damage" means any significant impairment to the:
(a) performance of a computer; or
(b) integrity or availability of data, software, a system, or information.

(5) "Execute," when used with respect to computer software, means the performance of the functions or the carrying out of the instructions of the computer software.

(6) "False pretenses" means the representation of a fact or circumstance that is not true and is calculated to mislead.

(7)
(a) "Identifying information" means any information that can be used to access a person's financial accounts or to obtain goods and services, including the person's:
(i) address;
(ii) birth date;
(iii) Social Security number;
(iv) driver license number;
(v) non-driver governmental identification number;
(vi) telephone number;

(vii) bank account number;
(viii) student identification number;
(ix) credit or debit card number;
(x) personal identification number;
(xi) unique biometric data;
(xii) employee or payroll number;
(xiii) automated or electronic signature;
(xiv) computer image file;
(xv) photograph; or
(xvi) computer screen name or password.

(b) "Identifying information" does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

(8) "Intentionally deceptive" means any of the following:

(a) an intentionally and materially false or fraudulent statement;

(b) a statement or description that intentionally omits or misrepresents material information in order to deceive an owner or operator of a computer; or

(c) an intentional and material failure to provide a notice to an owner or operator concerning the installation or execution of computer software, for the purpose of deceiving the owner or operator.

(9) "Internet" means the global information system that is logically linked together by a globally unique address space based on the Internet protocol (IP), or its subsequent extensions, and that is able to support communications using the transmission control protocol/Internet protocol (TCP/IP) suite, or its subsequent extensions, or other IP-compatible protocols, and that provides, uses, or makes accessible, either publicly or privately, high-level services layered on communications and related infrastructure.

(10) "Internet service provider" means:

(a) an Internet service provider, as defined in Section 76-10-1230; or

(b) a hosting company, as defined in Section 76-10-1230.

(11) "Message" means a graphical or text communication presented to an authorized user of a computer.

(12)

(a) "Owner or operator" means the owner or lessee of a computer, or a person using a computer with the owner's or lessee's authorization.

(b) "Owner or operator" does not include a person who owned a computer before the first retail sale of the computer.

(13) "Person" means any individual, partnership, corporation, limited liability company, or other organization, or any combination thereof.

(14) "Personally identifiable information" means any of the following information if it allows the entity holding the information to identify the owner or operator of a computer:

(a) the first name or first initial in combination with the last name and a home or other physical address including street name;

(b) a personal identification code in conjunction with a password required to access an identified account, other than a password, personal identification number, or other identification number transmitted by an authorized user to the issuer of the account or its agent;

(c) a Social Security number, tax identification number, driver license number, passport number, or any other government-issued identification number; or

(d) an account balance, overdraft history, or payment history that personally identifies an owner or operator of a computer.

(15) "Webpage" means a location that has a single uniform resource locator (URL) with respect to the World Wide Web or another location that can be accessed on the Internet.

Repealed and Re-enacted by Chapter 200, 2010 General Session

13-40-103 Application of chapter.

This chapter applies to conduct involving a computer, software, or an advertisement located in, sent to, or displayed in this state.

Enacted by Chapter 200, 2010 General Session

Part 2
Phishing and Pharming

13-40-201 Phishing and pharming.

(1) A person is guilty of phishing if, with intent to defraud or injure an individual, or with knowledge that the person is facilitating a fraud or injury to be perpetrated by another:

(a) the person makes a communication under false pretenses purporting to be by or on behalf of a legitimate business, without the authority or approval of the legitimate business; and

(b) the person uses the communication to induce, request, or solicit another person to provide identifying information or property.

(2) A person is guilty of pharming if, with intent to defraud or injure another, or with knowledge that the person is facilitating a fraud or injury to be perpetrated by another, the person:

(a) creates or operates a webpage that represents itself as belonging to or being associated with a legitimate business, without the authority or approval of the legitimate business, if that webpage may induce any user of the Internet to provide identifying information or property; or

(b) alters a setting on a user's computer or similar device or software program through which the user may search the Internet, causing any user of the Internet to view a communication that represents itself as belonging to or being associated with a legitimate business, if the message has been created or is operated without the authority or approval of the legitimate business and induces, requests, or solicits any user of the Internet to provide identifying information or property.

Repealed and Re-enacted by Chapter 200, 2010 General Session

13-40-202 Removal of domain name or content -- Liability.

If an Internet registrar or Internet service provider believes in good faith that an Internet domain name controlled or operated by the Internet registrar or Internet service provider, or content residing on an Internet website or other online location controlled or operated by the Internet registrar or Internet service provider, is used to engage in a violation of this part, the Internet registrar or Internet service provider is not liable under any provision of the laws of this state or of any political subdivision of the state for removing or disabling access to the Internet domain name or other content.

Repealed and Re-enacted by Chapter 200, 2010 General Session

13-40-203 Application of part.

(1) This part applies to the discovery of a phishing or pharming incident that occurs on or after July 1, 2010.

(2) This part does not apply to a telecommunications provider's or Internet service provider's good faith transmission or routing of, or intermediate temporary storing or caching of, identifying information.

Enacted by Chapter 200, 2010 General Session

13-40-204 Relation to other law.

The conduct prohibited by this part is of statewide concern, and this part's provisions supersede and preempt any provision of law of a political subdivision of the state.

Enacted by Chapter 200, 2010 General Session

Part 3
Spyware Protection

13-40-301 Prohibition on the use of software.

A person who is not an owner or operator of a computer may not cause computer software to be copied on the computer knowingly, with conscious avoidance of actual knowledge, or willfully, if the software is used to:

(1) modify, through intentionally deceptive means, settings of a computer controlling:

(a) the webpage that appears when an owner or operator launches an Internet browser or similar computer software used to access and navigate the Internet;

(b) the default provider or web proxy that an owner or operator uses to access or search the Internet; or

(c) an owner's or an operator's list of bookmarks used to access webpages;

(2) collect, through intentionally deceptive means, personally identifiable information:

(a) through the use of a keystroke-logging function that records all or substantially all keystrokes made by an owner or operator of a computer and transfers that information from the computer to another person;

(b) in a manner that correlates personally identifiable information with data concerning all or substantially all of the webpages visited by an owner or operator, other than webpages operated by the person providing the software, if the computer software was installed in a manner designed to conceal from all authorized users of the computer the fact that the software is being installed; or

(c) by extracting from the hard drive of an owner's or an operator's computer, an owner's or an operator's Social Security number, tax identification number, driver license number, passport number, any other government-issued identification number, an account balance, or overdraft history for a purpose unrelated to any of the purposes of the software or service described to an authorized user;

(3) prevent, through intentionally deceptive means, an owner's or an operator's reasonable efforts to block or disable the installation or execution of computer software by causing computer

software that the owner or operator has properly removed or disabled to automatically reinstall or reactivate on the computer without the authorization of an authorized user;

(4) intentionally misrepresent that computer software will be uninstalled or disabled by an owner's or an operator's action;

(5) through intentionally deceptive means, remove, disable, or render inoperative security, antispyware, or antivirus computer software installed on an owner's or an operator's computer;

(6) enable use of an owner's or an operator's computer to:

(a) access or use a modem or Internet service for the purpose of causing damage to an owner's or an operator's computer or causing an owner or operator, or a third party affected by that conduct, to incur financial charges for a service that the owner or operator did not authorize;

(b) open multiple, sequential, stand-alone messages in an owner's or an operator's computer without the authorization of an owner or operator and with knowledge that a reasonable computer user could not close the messages without turning off the computer or closing the software application in which the messages appear, unless the communication originated from the computer's operating system, a software application the user activated, or a service provider that the user chose to use, or was presented for any of the purposes described in Section 13-40-303; or

(c) transmit or relay commercial electronic mail or a computer virus from the computer, if the transmission or relay is initiated by a person other than the authorized user without the authorization of an authorized user;

(7) modify, without the authorization of an owner or operator, any of the following settings related the computer's access to, or use of, the Internet:

(a) settings that protect information about an owner or operator for the purpose of taking personally identifiable information of the owner or operator;

(b) security settings, for the purpose of causing damage to a computer; or

(c) settings that protect the computer from the uses identified in Subsection (6); or

(8) prevent, without the authorization of an owner or operator, an owner's or an operator's reasonable efforts to block the installation of, or to disable, computer software by:

(a) presenting the owner or operator with an option to decline installation of computer software with knowledge that, when the option is selected by the authorized user, the installation nevertheless proceeds;

(b) falsely representing that computer software has been disabled;

(c) requiring in an intentionally deceptive manner the user to access the Internet to remove the software with knowledge or reckless disregard of the fact that the software frequently operates in a manner that prevents the user from accessing the Internet;

(d) changing the name, location, or other designation information of the software for the purpose of preventing an authorized user from locating the software to remove it;

(e) using randomized or intentionally deceptive filenames, directory folders, formats, or registry entries for the purpose of avoiding detection and removal of the software by an authorized user;

(f) causing the installation of software in a particular computer directory or in computer memory for the purpose of evading an authorized user's attempt to remove the software from the computer; or

(g) requiring, without the authority of the owner of the computer, that an authorized user obtain a special code or download software from a third party to uninstall the software.

Repealed and Re-enacted by Chapter 200, 2010 General Session

13-40-302 Other prohibited conduct.

A person who is not an owner or operator of a computer may not, with regard to the computer:

(1) induce an owner or operator to install a computer software component onto the owner's or the operator's computer by intentionally misrepresenting that installing the computer software is necessary for security or privacy reasons or in order to open, view, or play a particular type of content; or

(2) use intentionally deceptive means to cause the execution of a computer software component with the intent of causing the computer to use the computer software component in a manner that violates any other provision of this chapter.

Repealed and Re-enacted by Chapter 200, 2010 General Session

13-40-303 Exceptions.

Sections 13-40-301 and 13-40-302 do not apply to the monitoring of, or interaction with, an owner's or an operator's Internet or other network connection, service, or computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service for network or computer security purposes, diagnostics, technical support, maintenance, repair, network management, authorized updates of computer software or system firmware, authorized remote system management, or detection or prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a network, service, or computer software, including scanning for and removing computer software prescribed under this chapter.

Enacted by Chapter 200, 2010 General Session

Part 4
Enforcement

13-40-401 Phishing and pharming violations.

(1) A civil action against a person who violates any provision of Part 2, Phishing and Pharming, may be filed by:
  (a) an Internet service provider that is adversely affected by the violation;
  (b) an owner of a webpage, computer server, or a trademark that is used without authorization in the violation; or
  (c) the attorney general.

(2) A person permitted to bring a civil action under Subsection (1) may obtain either actual damages for a violation of this chapter or a civil penalty not to exceed $150,000 per violation of Part 2, Phishing and Pharming.

(3) A violation of Part 2, Phishing and Pharming, by a state-chartered or licensed financial institution is enforceable exclusively by the financial institution's primary state regulator.

Repealed and Re-enacted by Chapter 200, 2010 General Session

13-40-402 Spyware protection violations.

(1) The attorney general, an Internet service provider, or a software company that expends resources in good faith assisting authorized users harmed by a violation of Part 3, Spyware

Protection, or a trademark owner whose mark is used to deceive authorized users in violation of Part 3, Spyware Protection, may bring a civil action against a person who violates Part 3, Spyware Protection, to recover:

(a) actual damages and liquidated damages of at least $1,000 per violation of Part 3, Spyware Protection, not to exceed $1,000,000 for a pattern or practice of violations; and

(b) attorney fees and costs.

(2) The court may increase a damage award to an amount equal to not more than three times the amount otherwise recoverable under Subsection (1) if the court determines that the defendant committed the violation willfully and knowingly.

(3) The court may reduce liquidated damages recoverable under Subsection (1) to a minimum of $100, not to exceed $100,000 for each violation, if the court finds that the defendant established and implemented practices and procedures reasonably designed to prevent a violation of Part 3, Spyware Protection.

(4) In the case of a violation of Subsection 13-40-301(6)(a) that causes a telecommunications carrier or provider of voice over Internet protocol service to incur costs for the origination, transport, or termination of a call triggered using the modem or Internet-capable device of a customer of the telecommunications carrier or provider of voice over Internet protocol as a result of the violation, the telecommunications carrier or provider of voice over Internet protocol may bring a civil action against the violator:

(a) to recover the charges the telecommunications carrier or provider of voice over Internet protocol is required to pay to another carrier or to an information service provider as a result of the violation, including charges for the origination, transport, or termination of the call;

(b) to recover the costs of handling customer inquiries or complaints with respect to amounts billed for the calls;

(c) to recover reasonable attorney fees and costs; and

(d) for injunctive relief.

(5) For purposes of a civil action under Subsections (1), (2), and (3), a single action or conduct that violates more than one provision of Part 3, Spyware Protection, shall be considered as multiple violations based on the number of provisions violated.

Enacted by Chapter 200, 2010 General Session